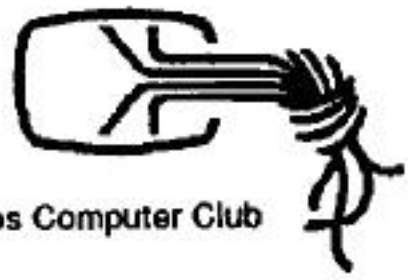
Die Datenschleuder



Das wissenschaftliche Fachblatt für Datenreisende Ein Organ des Chaos Computer Club

ISSN 0930 - 1045 Mai 1994 Nr. 47 DM 3,50

»Hasta la Villa, Baby!«

Die Villa, das ist Cyberspace im Telefon – ein weltweit einmaliger akustischer Abenteuerspielplatz für Kinder ab 18. Und das heißt: Flirten statt Warten!

Tag und Nacht amüsieren sich Dutzende von Leuten miteinander in der Villa. Denn hier kann jeder Anrufer live und sofort mit jedem reden! Wann immer Du anrufst, Du wirst nicht allein sein auf Deiner Reise durch das schöne Haus. Und auf den drei Etagen gibt es viel zu entdecken:

Man kann ungestört zu zweit in der Badewanne planschen oder auf dem Sofa kuscheln, oder Du liest im Gästebuch oder schreibst Deine Kontaktanzeige auf die Tischdecke...

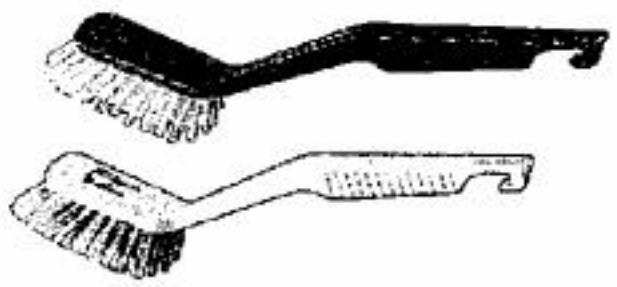
Die Antworten bekommst Du auf Deinen Schreibtisch**, den Du gratis aufstellen kannst. Zieh zu uns in die Villa!

Du brauchst nur einen Nummernpiepser (vom Anrufbeantworter) oder ein Telefon, auf dem Du die Tasten → * → drückst.

Kostenlose Informationen unter
0130/800 337 und
Btx *655324#

Und dann auf in die Villa:
0190/577 995*

Audioland/AIKIU *(0,23 DM/12 Sek.) **Hotline 01805/221 227



0130er auf ISDN-Basis digitalisiert

(crd/05.05.1994) – Die bisher "analogen" Service-130 Vermittlungen sind offenbar digitalisiert worden.

Zumindest im Norddeutschen bekommen die Inhaber von 0130-Rufnummern seit einigen Tagen die OAD (*originating Adress* = Ursprungstelefonnummer) von ISDN-Teilnehmern angezeigt. Abgesehen von hierbei aufkommenden Fragen des Datenschutzes, muß auch die Frage nach dem Sinn dieser sicherlich kostspieligen Maßnahme gestellt werden. Denn mit dieser lassen sich nicht nur Kundenrückrufe erleichtern, sondern auch Rückverfolgungen problemlos starten. Auch bei "normal" digital vermittelten Teilnehmern läßt sich die Ursprungstelefonnummer problemlos erfassen, bei Teilnehmern an alten, analogen Ämtern zumindest die Ortsnetzkennziffer. Inwieweit dies mit Maßnahmen zur Netzsicherheitssimulation bzw. Einschränkung des Mißbrauchs von 0130-Rufnummern zusammenhängt, konnte noch nicht recherchiert werden. In Telekom-Kreisen waren in letzter Zeit Informationen über einen anonymen Anrufer von 0130-Rufnummern bekannt geworden, der die für die ankommenden Rufe bezahlenden Anbieter viel Geld durch computergestützte massenhafte Anrufe mit baldiger Verbindungsauslösung (Auflegung) verursacht. Dies, also systematisch falsches Wählen, stellt allerdings keine Straftat oder ähnliches dar.

Filename: CRD94051.D47 Last edit: 9405072140

Autor: Andy/CRD

Der in dieser Ausgabe dokumentierte "Yellow-Point" CD-ROM Hack hat zu einer unerwarteten Resonanz geführt. Seit Bekanntwerden klingelt in den Hamburger Clubräumen fast ununterbrochen das Telefon; ob wir nicht mal eben die Codes durchgeben könnten. Können wir selbstverständlich nicht - aus zwei Gründen. Zum einen wollten wir die uns angedrohten Schadensersatzforderungen nicht unbedingt riskieren, zum anderen ist es nur bedingt in unserem Interesse. Denn bei der Veröffentlichung des Hacks ging es uns ja nicht darum, die auf dieser CD-ROM enthaltene Software jedem umsonst zugänglich zu machen, sondern ganz generell die Softwareindustrie zum Nachdenken über die Preisgestaltung beim Softwarevertrieb zu bringen. Denn die Tatsache, daß fast jeder Computerbenutzer in Deutschland ein Straftäter wegen Urheberrechtsverletzung ist, ist nicht länger akzeptabel. So ist es seit neuestem gang und gebe, daß Computerbenutzer, deren Computer aus einem beliebigen Grunde von der Polizei beschlagnahmt wird, zusätzlich noch ein Ermittlungsverfahren wegen Verstoß gegen das Urheberrechtsgesetz angehängt bekommen. Durch die Novellierung des Urheberrechtsgesetzes (EG-Vereinheitlichung) ist das jetzt Straf- und nicht mehr nur Zivilrecht.

So bitten wir also die vielen Interessierten, die uns 10.- DM für ein Probeabonemment der Datenschleuder geschickt haben - in der Hoffnung auf "die Codes" - um Verständnis, hier nur ein Schema präsentieren zu können. Wie dem "Spiegel" vom 2.5.94 zu entnehmen war, hat mittlerweile ein Bösewicht namens "Interzeptor" eine Software in die Datennetze gepumpt, die das Entschlüsseln der CD-ROM erlaubt. Hiervon möchten wir uns natürlich ganz herzlich distanzieren.

Mit freundlichen Grüßen,
euer Chaos-Team

Die Geschichte mit der "Yellow-Point" CD-ROM

kurze Übersicht über die Ereignisse

Bereits seit der DAFTA (Datenschutzfachtagung) im November 1993 waren die grundlegenden Informationen über die Unsicherheit des z.B. von der Yellow-Point verwendeten Software-Verschlüsselungs-Verfahrens bekannt (siehe Diagramm). Zur CeBit begab es sich dann, daß die CD-ROM zunächst zusammen mit der Zeitschrift "PC-Direkt" herauskam, um dann schliesslich auf der CeBit verschenkt zu werden. Die prinzipielle Unsicherheit des Systems in Verbindung mit den zusätzlich hier vorhandenen Programmier-Bugs (Fehlern) ermöglichte es, die auf der CD-ROM verschlüsselte Software in weniger Zeit zu entschlüsseln, als für den Transport zu unseren Mitgliedern nach Bulgarien notwendig war.

Am Samstag morgen wurde zunächst versucht, einen Verantwortlichen bei Yellow-Point zu erreichen. Dies scheiterte schon im Ansatz: am Telefon konnte oder wollte man noch nicht einmal den Namen des Geschäftsführers oder eines Verantwortlichen nennen. Die CD-ROMs wurden immer noch verschenkt, so dass sich einige anwesende Chaoten entschlossen, eine Meldung auf die Netze und an eine Nachrichtenagentur zu schicken. Samstag nachmittag ging die Geschichte dann als dpa-Meldung über die Ticker und es entstanden Radio- und Zeitungsbeiträge. Ein bereits vorher entstandener Fernsehbeitrag wurde von der ARD - obwohl gekauft - nicht gesendet; man befürchtete rechtliche Konsequenzen, das sei ja "mehr oder weniger ein Aufruf zum Raubkopieren"

Ob es an unserer Meldung oder der Verkürzung von DPA lag: die Darstellung des eigentlichen Problems misslang etwas. In erster Linie kam die Meldung "CCC knackt CD-ROM" und nicht "CCC weist auf Probleme beim Softwareverkauf hin". Liegt natürlich auch daran, daß sich letzteres schlechter verkauft. Es ist längst bekannt, dass auf ein Stück legal erworbene Software viele tausend Stück Kopien kommen. Aber anstatt, wie beim Shareware-Konzept, hier mit alternativen Lösungsmöglichkeiten den Ausweg aus der Misere zu suchen, setzen die konventionellen Softwareproduzenten auf Einschüchterung (siehe auch 0130-4011, dazu demnächst mehr) und "easy to buy" - Konzepte à la Yellow-Point.

Das Problem bleibt: private Kunden sind weder dazu bereit noch in der Lage, Software zum Preis von Produktionsmitteln zu kaufen - lernorientierte jugendliche Computerbenutzer schon gar nicht. Hier nützen Demo-Versionen mit beschränktem Funktionsumfang (wie bei einem bekannten Textbearbeitungsprogramm, in dessen Demoversion die Speicherfunktion gesperrt ist, die in der Vollversion aber leider auch nicht richtig funktioniert) am wenigsten. Demoversionen mit Zeitbeschränkung erlauben zwar eine bessere Einsch ätzung, ob die Software denn die ist, die man braucht, senken die Preise aber auch nicht auf ein verträgliches Niveau.

Die Geschichte mit der "geknackten Yellow-Point-CD-ROM" hat die Softwaredistributoren und Produzenten sicherlich verschreckt. Ein Informationsfluss zwischen CCC und Yellow-Point lief zunächst über Journalisten. Als es hiess, die Firma Yellow-Point werde von jemandem, der sich als CCC'ler auswies, erpresst, der damit drohte, die Codes freizugeben, wenn nicht ein bestimmter Betrag gezahlt werde, änderte sich dies. Der zunächst koopera-

tive Pressesprecher verwies auf den Geschäftsführer von Yellow-Point bzw. auf den verantwortlichen Projektleiter. Diesem wurde erläutert, dass der CCC kein Interesse und nicht die Absicht habe, das Unternehmen zu erpressen oder überhaupt die "Codes" herauszugeben. Dem CCC ging es um die Unsicherheit des Systems (Sicherheit ist eine Illusion) und um die Diskussion des ganz alltäglichen Wahnsinns, Softwarevermarktung genannt. Letztlich muss es zu einer Lösung kommen, die auch für minder finanziell ausgestattete Computerbenutzer befriedigend ist.

In Köln fand ein Treffen zwischen Mitgliedern des CCC, dem verantwortlichen Projektleiter und dem Programmierer der Fa. Yellow-Point statt, bei dem in einem konstruktiven Dialog die Geschichte, ihre Folgen, Hintergründe und Lösungsansätze diskutiert wurden. Yellow-Point, so der Leiter des Projektes, Herr Schneider, habe keinen wirklichen Schaden von der Geschichte erlitten. Der Kontakt zu den Softwareproduzenten sei eng genug, die CD-ROM verkaufe sich besser als vor den Pressemeldungen und überhaupt habe man damit gerechnet, dass das Verfahren knackbar sei. Ausserdem seien die von der CD-ROM kopierten Programme ja Raubkopien wie andere auch.

Die Frage, ob man denn das Wissen um den 1 Byte DES-Code und den 6-Iterationen-DES nicht unter den Tisch fallen lassen könne, konnten wir leider nicht bejahen (Freedom of Information contra security by obscurity).

Dies, oder irgend etwas anderes, haben uns die Herren vermutlich übel genommen. Nach dem eigentlich konstruktiven Kölner Gespräch waren wir zunächst erstaunt, von einem recherchierendem Journalisten zu hören, Yellow-Point habe einen bekannten, in München ansässigen Anwalt beauftragt, gegen den CCC, den Schreiber diesen Artikels (der auch auf dem Kölner Treff war) sowie gegen Josef Bugovics, der bereits auf der Dafta '93 über die Unsicherheit dieses Distributionskonzeptes berichtet hatte, vorzugehen.

Besagter Anwalt war nur bedingt für eine Stellungnahme zu gewinnen, verwies jedoch auf die gemeinsame Streitkultur, war er doch nicht zuletzt regelmäßiger Besucher des Chaos Communication Congress - der Bösewicht sei Josef Bugovics. Herr Schneider, der Verantwortliche bei Yellow-Point, war ab diesem Zeitpunkt telefonisch leider nicht mehr zu erreichen. Die Sekretärin der Fa. Yellow-Point verwies auf Besprechungen, wann immer man auch anrief. Zwischenzeitlich lies Herr Schneider ausrichten, dies sei nicht als Abbruch der diplomatischen Beziehungen zu werten. Er sei auch nach wie vor an den vorgeschlagenen Shareware-Konzepten interessiert.

Ein Vertreter einer Firma, die international Büromaschinen vertreibt und in Anzeigenkampagnen gerne die Behauptung aufstellt, die besten Hacker säßen... bei ihnen, fragte dann noch an, ob denn der CCC eine Untersuchung des von ihnen verwendeten (Verschlüsselungs-)Verfahrens durchführen könne. Allerdings erreichte dieser Mensch den CCC'ler zwischen Strassenbahn und Haustür, so dass um schriftliche Anfrage per Fax gebeten wurde. Das kam dann allerdings nicht, dafür einige Wochen später ein Anruf von selbiger Firma mit selbigem Anliegen, allerdings etwas gewähltere Sprache, vermutlich eine Etage höher ansässig als der vorherige Anrufer. Dafür, daß der CCC sich nicht als Dienstleistungsunternehmen zur Verfügung stelle, habe man ja Verständnis, ob denn nicht gegen eine Spende eine Untersuchung mit exklusiver Ergebniskanalisierung... doch auch dieser Herr genierte sich offenbar zu sehr, als das er diese Anfrage faxen konnte. Frei nach dem Motto: die besten Hacker sitzen zwar nicht bei uns, aber neulich haben wir sie mal

angerufen.

Quintessenz: für die Untersuchung irgendeines Produktes steht der CCC als Dienstleistungsunternehmen sicherlich nicht zur Verfügung. Solch ein Projekt ist nur vorstellbar, wenn die gewonnenen Erkenntnisse dann auch veröffentlicht werden können, um der allgemeinen Evolution zu dienen, statt sich für ein Unternehmen exclusiv zu prostituieren.

Die Mißstände beim Verkauf von Software – ganz allgemein, werden aber sicherlich nicht durch sicherere Verschlüsselungs-Konzepte behoben. Irgendwann werden das auch die Produzenten begreifen, genauso, dass man Geld nicht essen kann. Hoffentlich, bevor der letzte Baum...

Andy

Filename: YPALLG.D47 Lastedit: 9405132130
Autor: ANDY

Software-Klauf ◀bequem wie nie

Schema der Verschlüsselung von PAY-CD-ROMs

- Produktionsverfahren:

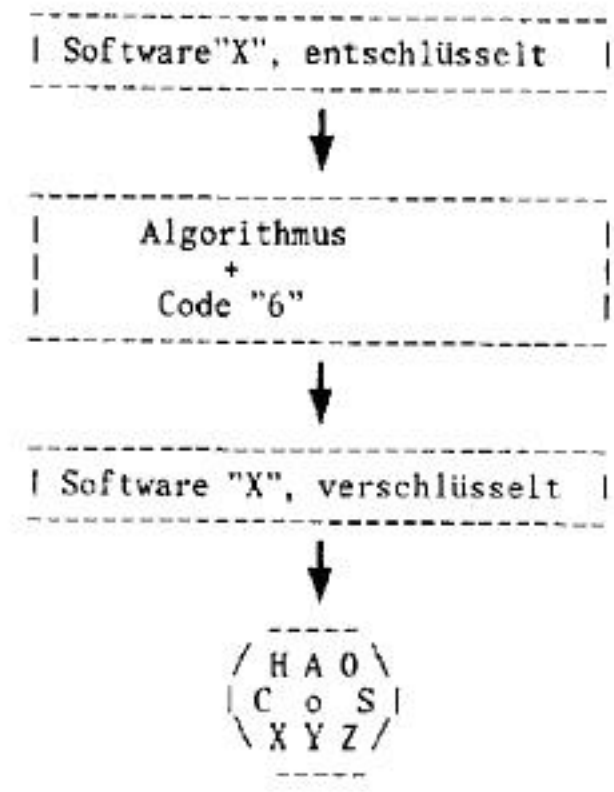
Die entschlüsselte Software "X"

wird mit einem Verschlüsselungs-
sowie
einem hierzu gehörigen Code
verschlüsselt (z.B. "6")

und dann...
zusammen mit der anderen Software

(jede Software ein eigener Code)
auf die CD-ROM
gepackt

Diese CD-ROM wird (weil eine Einzelfertigung zu teuer ist) 300.000 mal kopiert.



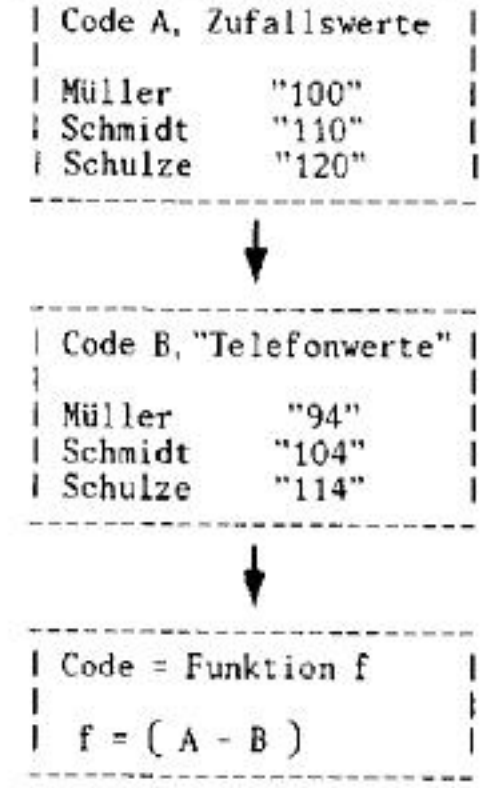
- "Kaufen einer Software"

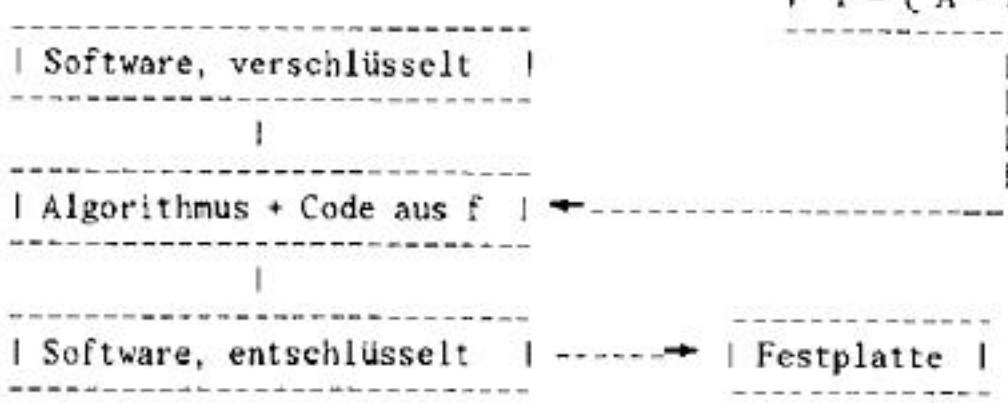
Der Kunde ruft die Auspacksoftware auf der CD-ROM auf, und entschliesst sich, Software "X" zu kaufen. Er klickt diese mit der Maus an, und bekommt auf den Bildschirm die Telefonnummer der Abwicklungs-Firma X. Dieser gibt er seine Kreditkartennummer, seinen Namen und Anschrift sowie eine auf dem Bildschirm erscheinende Buchstaben/Zahlenkombination A

Nach der Prüfung der Kreditkartennummer erhälten die Kunden dann am Telefon den Bestandteil B genannt, siehe Diagramm.

Die Software errechnet sodann aus A und B mit der Funktion f den Entschlüsselungs-Code.

Dieser geht dann wieder in den Algorithmus ein, der die Software entschlüsselt.



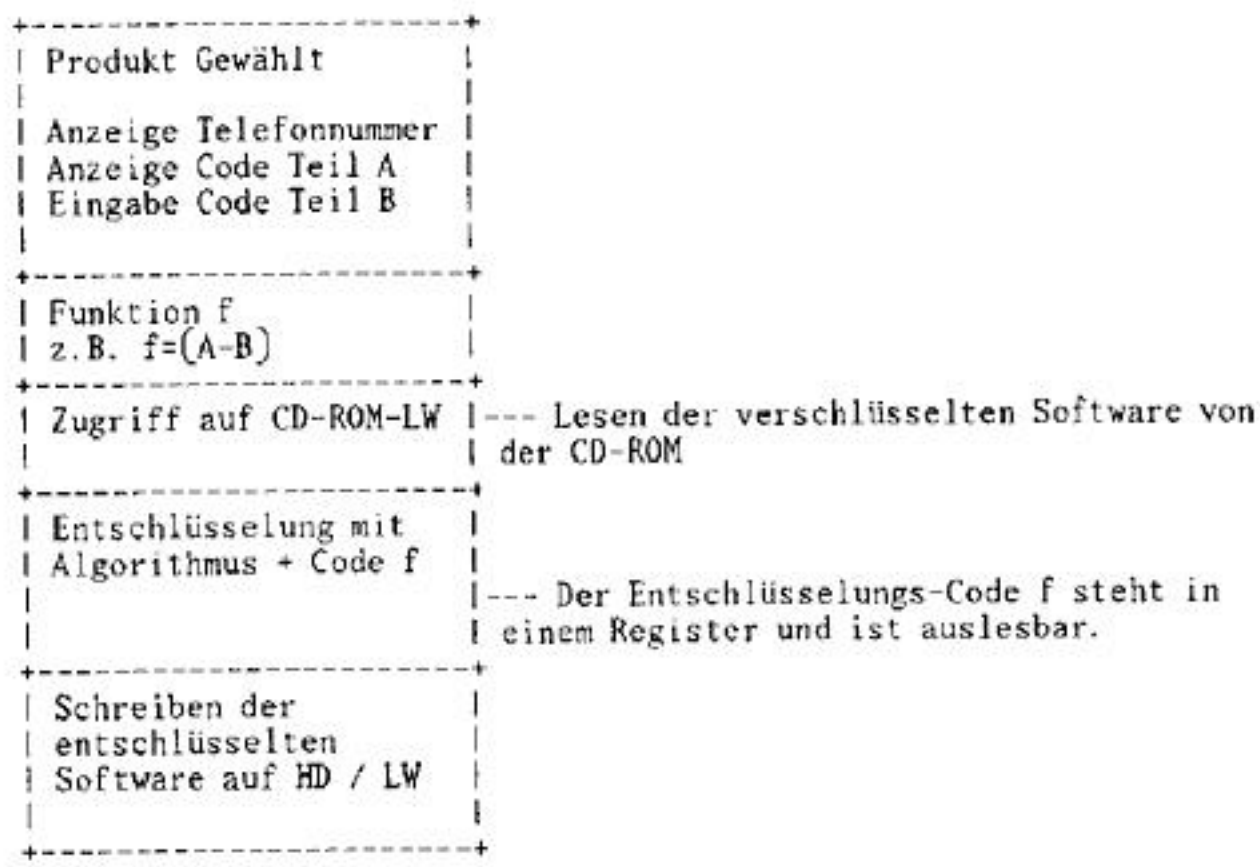


... die der Kunde sich dann auf seine Festplatte bzw. auf Disketten kopieren darf (bekommt Diskettenaufkleber + Handbücher zugeschickt).

Übrigens: Bei dem hier dargestellten Verfahren ist die CD-ROM ja eine 300.00fach kopierte ist, ohne das über die durchgegebenen Zahlenkolonnen eine Seriennummer gebildet würden. Eine Rückverfolgung einer Raubkopie mittels Seriennummer ist hier also mangels dieser eher nicht möglich.

Das Entscheidende ist, daß, egal wie kompliziert die Funktion f aus A und B auch immer sein mag, das Ergebnis der Entschlüsselungscode ist, der in den Ver-/Entschlüsselungsalgorithmus (hier: DES) eingehen muß.

In irgendeinem Register X muß also immer der Entschlüsselungscode vorliegen, so daß es möglich ist...



...den Code auszulesen.

- "Klau-Methode"

Mit einem virtuellen Debugger lassen sich also zunächst in Bulgarien (das ist dort legal, in der BRD würde es eine vermutlich eine Rückentwicklung darstellen, die nach Paragraph 69c nur mit Zustimmung des Programmerstellers zulässig wäre) die Register beobachten, um dann den Entschlüsselungs-Code beim "legalen" Kauf einmal auszuspähen. Es ließe sich ein Programm schreiben, um den Entschlüsselungs-Code in einer extra-Datei abzuspeichern.

Mit einer weiteren Software wird dann die "Telefonzahlenspielerei"- Prozedur umgangen, und der jeweilige Entschlüsselungs-Code direkt in das Register des Algorithmus geschrieben.

Jede Software muß zwar nach dieser Methode 1 mal "legal" gekauft werden, um den Code auszuspähen, aber mit diesem Prinzip läßt sich jede (!) CD-ROM, die nach diesem Verfahren arbeitet "knacken", egal wie kompliziert die Funktion f und der Verschlüsselungs-Algorithmus ist. Über die bekannten Möglichkeiten der Vernetzung von Computern würden sich die "Schlüssel" zu Listen zusammenfassen und verbreiten lassen. Bis

hierhin geht es also um die grundzipielle Unsicherheit von PAY-CD-ROMs, wie sie Josef Bugovics auf der Dafta im November 1993 erläutert hat. Nach diesem Verfahren wäre es also möglich gewesen, die CD-ROM zu knacken, gäbe es nicht noch einige ...

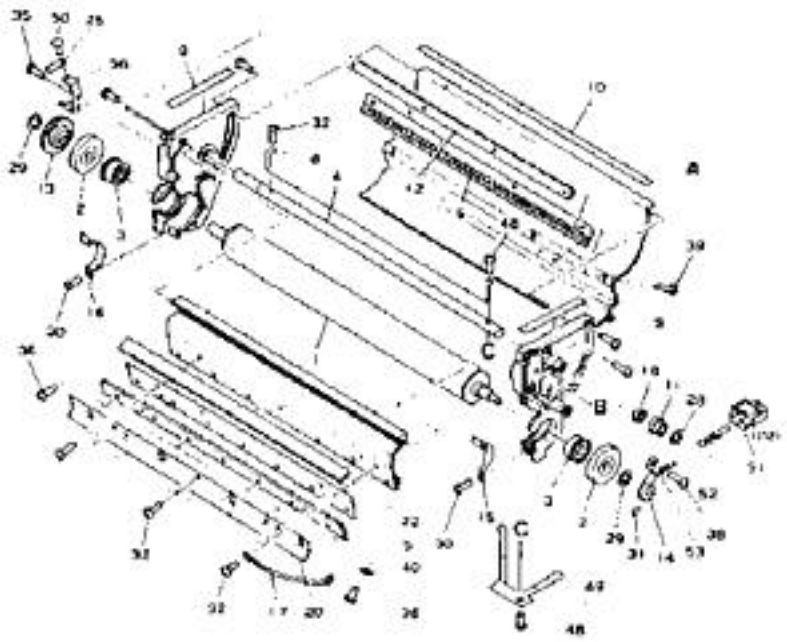
- Besonderheiten bei "Yellow Point"

Bei der von der Firma "Yellow Point" verbreiteten CD-ROM wird ein DES-Algorithmus verwendet. Ein DES-Algorithmus (genauer Aufbau in einer der nächsten Datenschleudern) besteht im Groben aus einer Formel und einer Tabelle. Der Algorithmus wird mit den Werten der Tabelle je nach Länge dieser n-mal angewendet. Beim DES ist die Anzahl dieser Rechenschritte, die "Iterationen", normalerweise 16. Um Rechenzeit zu sparen, wurde bei "Yellow Point" jedoch ein DES mit nur 6 Iterationen verwendet. Die Sicherheit des DES verhält sich allerdings exponentiell zu der Anzahl der Iterationen. Für einen DES mit nur 6 Iterationen sind allerdings Methoden bekannt, ihn zu "knacken" (auch hierzu mehr in einer der nächsten DS).

Damit wäre der Aufwand "Yellow-Point" zwar schon ein geringerer, es kommt allerdings noch besser: durch programmiertechnische Absonderlichkeiten beträgt die Schlüssellänge genau 1 Byte. Das bedeutet, es gibt 256 verschiedene Möglichkeiten der Entschlüsselung pro Software der CD-ROM. Damit schrumpft der Aufwand, alle Möglichkeiten auszuprobieren auf ein Programm von wenigen K.

Ohne ein Netzwerk von Mitgliedern, das sich bis nach Bulgarien erstreckt, wäre zwar auch das Herausfinden dieser programmiertechnischen Besonderheiten womöglich ein Verstoss wie o.g. gegen das Urheberrechtsgesetz gewesen. Nachdem die dort erlangten Informationen jedoch bekannt waren, stellte sich vielmehr die Frage, ob es sich hier nicht womöglich um eine fahrlässige Verbreitung von nichtlizensierter Software handelte.

Filename: YPSCHEMA.D47 Lastedit: 9405072158 Autor: AND



Der Chaos Computer Club empfiehlt:

Volkspreis

für die 2 MioBit-Telefonmaschine!

Erst bei einer Grundgebühr von deutlich unter 100 DM pro Monat kann die zentrale digitale Telefonschnittstelle der europäischen Zukunft, der bidirektionale 2 MB-Anschluß, seine technische Innovationskraft entfalten und Deutschland ein wenig aufholen im Weltmaßtab.

Denn nicht nur Deutschland, sondern ganz Europa liegt digital international zurück. Schuld daran ist nicht zuletzt das planwirtschaftliche Vorgehen von Bangemann und Konsorten in Brüssel und Bonn. Diese D2-MACker führten mit staatlichen Zwangsmaßnahmen veraltetes Analogfernsehen ein, statt digitale Zukunfts-Techniken bei Telefon, Hörfunk und Fernsehen zu fördern. Auch der frühere Postminister hat von der digitalen Revolution nur wenig mehr als eine Bleibatterie verstanden, aber mit diesem marktwirtschaftlichen Basiswissen hat er immerhin eine gewisse De-Regulierung geleistet (*dafür* sei ihm gedankt). Doch der jetzige Postminister sollte dieses Papier besser dem Wissenschaftlichen Dienst des Bundestages und auch seinen Beratern und Redenschreibern zum Lesen geben :-)

Zum Aufholen im internationalen Wettbewerb brauchen wir Datenautobahnen in Deutschland, und zwar zu Gebühren, die es nicht nur Mercedesfahrern erlauben, sie zu benutzen.

Die Voraussetzungen sind gegeben, weil in fast jeden Haushalt vier Kupferdrähte führen. Die Post weiß, daß die Kabel das Teuerste sind - ihre Milliardenverluste beim Verbuddeln von Ein-Weg-Koaxkabel belegen das öffentlich. Und schon jetzt reicht die Verteil-Kapazität des Koaxkabels nicht einmal für die vorhandenen Fernsehprogramme, um von den digitalen Fernsehsatelliten zu schweigen. Zwar verlegt die TELEKOM in Deutsch-Nahost schon die Röhren für die Glasfasern parallel zu den Telefonkabeln, aber das hilft jetzt nicht, und in West-D auch nicht.

Was wir heute brauchen, sind keine Koaxkabel und keine Glasfasern in jede Wohnung, sondern 2 Miobit/Sekunde über real existierende Drähte zu einem anständigen Preis. Mit MPEG2 kann darüber ein Fernsehprogramm in guter Qualität übertragen werden oder sonstige Daten. Zum Aufholen im Weltwettbewerb hilft aber nur Praxis und zwar im großen Maßstab. Dann hat Deutschland eine Chance, durch Entwicklung von Applikationen und Software und praktische Erprobung den Entwicklungsvorsprung der USA, die schon einen Digitalsatelliten oben haben, zumindest auf der Erde ein wenig aufzuholen.

Die Zeiten der Forderungen sind vorbei.

Der Chaos Computer Club empfiehlt das nur im Rahmen seiner Lobbyarbeit öffentlich zur CeBIT 1994. Eine Empfehlung reicht und die Regierung muß reagieren, und sei es erst die nächste oder die übernächste. . . Langfristig denken und gleich handeln und Akten schaffen ohne Waffen!

Kommunikationspreise sind politische Preise! Wann ist Schluß mit der Beutelschneiderei an der Datenautobahn? *Runter von den Datenfeldwegen und rauf auf die Datenautobahn!* Sie existiert ja eigentlich schon - nur der Preis ist zu heiß!

Pressure Group verantwortlich: Wau Holland, Alterspraesident Chaos Computer Club Das sofortige Bebrueten & Verwerten dieses Materials ist erwünscht - schneller brüten bitte! (Der CCC ist eingetragen in der Lobbyliste des Deutschen Bundestages.) Wau ist zu erreichen in der Arnstädter Str. 26/7, D - 98 693 Martinroda / Thüringen.

Filename: WAUTEL.D47 Lastedit: 9405072150

Autor: WAU

Anrufbeantworter abhören

Manchmal ist es schon paradox ... bei Rechnern machen Hersteller und Betreiber einen Riesenaufwand, um unberechtigten Zugriff auf Informationen zu verhindern, auf der anderen Seite sind Geräte, auf denen sicher auch relevante Informationen liegen können, nämlich Anrufbeantworter, oft nicht oder fast nicht geschützt. Auch bei heute gängigen Modellen finden sich Fernabfragecodes, die entweder gar nicht veränderbar sind, die nur aus wenigen Möglichkeiten ausgewählt oder die mit zwei bis drei Stellen leicht durch Trial&Error geknackt werden können. Da die meisten Geräte nach Fehleingaben höchstens auflegen, aber nicht abschalten, kann man quasi beliebig oft ausprobieren. Wenn man dann noch hergeht und die zu testenden Zahlenkombinationen durch geschickte Wahl der Ziffernkombinationen zusammenfasst, kommt man noch schneller ans Ziel. Daß triviale Kombinationen wie '000' oder '123' besonders beliebt sind, braucht glaube ich nicht extra erwähnt zu werden ;-)

Nachdem man den Code einmal gefunden hat, sind mit einigen Versuchen und Kenntnis der wichtigsten Gerätegrundtypen schnell die wesentlichen Funktionen des Gerätes herausgefunden, und man kann nach al gusto Nachrichten abhören, diese löschen, Ansagetexte verändern oder mittels Raumüberwachungsfunktionen testen, ob jemand zu Hause ist. Zu den besonders unsicheren Geräten gehören beispielsweise Anrufbeantworter von Sanyo oder 'Assmann Computer', die lediglich Codes im Bereich 11-19 zulassen. Viel besser sieht es auch nicht bei Modellen wie denen von DSC aus. Hier kann man eine Auswahl aus 10 festeingestellten Kombinationen treffen. AT&T

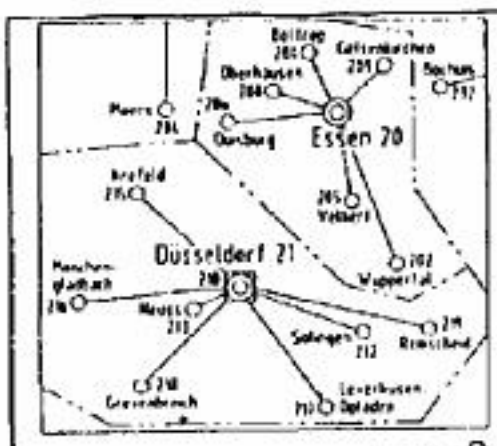
Why we see news anchorpersons only from the waist up.~,

ist da mit zweistelligen Codes schon geradezu vorbildlich. Von Cod-a-phone kommen in der Regel Geräte, die durch einen dreistelligen schon besser geschützt sind.

Pseudedreistellige Codes wie bei Panasonic, wo die ersten beiden Ziffern fest vorgegeben sind und nur die letzte eingestellt werden kann, sind IMHO ein schlechter Witz. Geräte wie von Tiptel oder auch der baugleiche Rispondo von der Telekom haben immerhin auch einen dreistelligen Code und legen nach 3 Fehlversuchen auf. Damit wird ein Hackversuch zumindest mal teurer, als wenn wenige Anrufe genügen, um eine Vielzahl Kombinationen auszuprobieren. In diesem redigierten Artikel hab ich mal alle Geräte aufgenommen, die mir so untergekommen sind. Die unterschiedlichen Geräte der Hersteller unterscheiden sich in der Regel nicht bzgl. ihres Fernabfrageverhaltens, so daß es gar nicht soviele unterschiedliche gibt.

Ciao ... Frank

ComRam = Frank Kargl



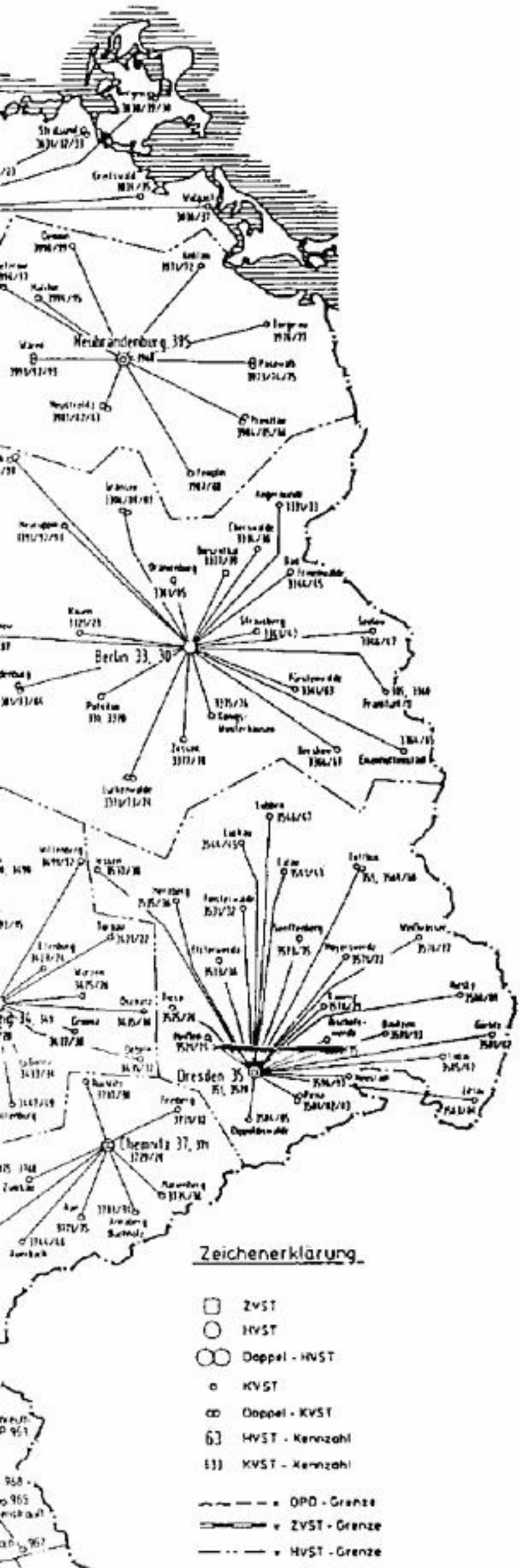
Ausschnitt:

HVSt-Bereiche
Düsseldorf 21 und Essen 20

Nordsee

Ostsee

Flensburg 45
Heide 48
Kiel 43
Lübeck 45
Rostock 38
Hamburg 41
Bremerhaven 47
Leer 49
Oldenburg 44
Bremen 42
Uelzen 58
Lingen 59
Osnabrück 56
Minden 57
Hannover 51, 59
Braunschweig 53
Magdeburg 391
Bielefeld 52
Münster 25
Wesel 28
Dortmund 23
Essen 20
Düsseldorf 21
Hoscheide 29
Göttingen 55
Kassel 56
Erfurt 36
Köln 22
Siegen 27
Aachen 24
Gießen 64
Fulda 66
Koblenz 26
Frankfurt 61
Main 60
Bad Kissingen 97
Würzburg 93
Bamberg 95
Bayreuth 92
Trier 65
Bad Kreuznach 67
Mannheim 62
Nürnberg 91
Weiden 96


Neubrandenburg 395
Berlin 33, 30
Dresden 35
Chemnitz 37, 371
Zeichenerklärung
ZVST
HVST
Doppel - HVST
KVST
Doppel - KVST
63 HVST - Kennzahl
633 KVST - Kennzahl
OPD - Grenze
ZVST - Grenze
HVST - Grenze

"Von außen eingespielt"

Zu den Hausdurchsuchungen in Bielefeld und Göttingen wegen einer elektronischer Anleitung zu pyrotechnischen Experimenten und wer dahinter stecken könnte

7. April 1994: In den Räumen der Mail-Box //BIONIC (betrieben von der mit dem CCC befreundeten Organisation FoeBuD e.V.) trafen pünktlich zum Beginn der Geschäftszeit Beamte der Staatsschutzabteilung der Bielefelder Polizei und Computerexperten des BKA ein. Sie hatten etwas Nettes für die Mieterin und den Mieter der ehemaligen FoeBuD-Räume mitgebracht: einen Hausdurchsuchungsbefehl.

"Der Verdacht, daß die Betroffenen Beweismittel, nämlich Unterlagen über die Druckschriften 'Der kleine Terrorist' und 'Eine Bewegung in Waffen, Band IIb, Handbuch für improvisierte Sprengtechnik, Hg.: Autorenkollektiv Werwolf' in ihrem Besitz haben, ergibt sich aus den vorgelegten Ermittlungsakten, insbesondere aus Zeugenaussagen / polizeilicher Spurensicherung und anderen Indizien", stand auf dem Blatt zum Ermittlungsverfahren wegen "Störung des öffentlichen Friedens".

padeluun, Medienkünstler und einer der Betreiber der //BIONIC, auf den auch der Durchsuchungsbefehl ausgestellt war, begrüßte die Beamten freundlich und bat ihnen einen Stuhl an. Die Durchsuchung hatten eigentlich schon alle seit einem halben Jahr erwartet. Der Text "Der kleine Terrorist" war auf die Bitte des Autors in der //BIONIC schon gelöscht worden. Er beschrieb sorgfältig die Herstellung verschiedener militärischer Sprengstoffe, gab eine Anleitung zum Bau von Briefbomben und Tips zur Verarbeitung von brisanten Materialien aus dem Gärtnerbedarf zu Plastiksprengstoff. Information soll bekanntermaßen frei sein. Deshalb wurde auch letztes Jahr im MailBoxverbund Z-NETZ das Brett /T-NETZ/PYROTECHNIK eingerichtet, in dem allerdings im ersten Text auf bestehende Gesetze hingewiesen wurde, wenn auch mit einer Einschränkung: "Im Zweifelsfalle gilt die Hackerethik".

Weiterleitung: "Der kleine Terrorist" geht nach Thule

Richtig brenzlig wurde die Sache erst, als im Thule-Netz, einem von verschiedenen faschistischen Organisationen der "nationalrevolutionären" Prägung getragenen Netzwerk (unter den gestrengen Augen des Verfassungsschutzes) diese Anleitung von dem Thule-Teilnehmer NPD-BTX-ZEITUNG eingespielt wurde. Wie bei elektronischer Vernetzung üblich, geschah dies von außen, versehen mit dem nationaldemokratischen Zusatzvermerk "Seht mal, was die Linksrassisten [sic!] im ComLink da so machen!". Offenbar hatten die Deutschländerwürstchen mitbekommen, daß die //BIONIC auch im Frieden-, Umwelt- und Menschenrechte-Netzwerk /CL mitarbeitet (neben den GRÜNEN, der SPD, der PDS, Greenpeace, dem BUND und von Zeit zu Zeit auch der CDU).

Da diese NPD-Aktion in einer Zeit geschah, in der "Nazi-Vernetzung" auf allen Kanälen Medienaufmerksamkeit bekam, mußten die offiziellen Stellen wohl Ermittlungen einleiten und spielten das Spiel nach den von der NPD vorgegebenen Spielregeln mit. Besonders schön spielte hier das Oberlandesgericht Nürnberg in einer Presseerklärung im Januar: "Nach bisherigen Erkenntnissen wurde der Text [...] von *außen* in die Erlanger MailBox [gemeint ist das Thule-System WIDERSTAND von T. Hetzer, Herausgeber der Zeitschrift "Saufeder" der Jungen Nationaldemokraten] eingespielt; von wem, ist noch nicht abschließend geklärt." Der Absendername NPD-BTX-ZEITUNG im Nachrichtenkopf war für die fränkischen Ermittler anscheinend nicht zu lesen...

Bitte recht freundlich!

Zurück zur Hausdurchsuchung: Da für die neuen FoeBuD-Räume kein Durchsuchungsbefehl vorlag, gab es zunächst einige Schwierigkeiten, an die gewünschten Daten zu kommen (das "Handbuch für improvisierte Sprengtechnik" der amerikanischen NSDAP/AO lag allerdings gleich griffbereit, es war durch die Redaktion der WDR-Sendung ZAK in den FoeBuD-Besitz gekommen, was den Beamten dann auch freundlich erklärt wurde).

Nachdem seltsame Wünsche wie die Herausgabe aller Userdaten abgewendet werden konnten, wurde schließlich der Inhalt des Brettes /T-NETZ/PYROTECHNIK auf Band kopiert. Die MailBox wurde nicht mitgenommen, was wohl der Tatsache zu verdanken ist, daß padeluun darauf hinwies, daß im arbeitenden Redaktionssystem //BIONIC ein solcher Eingriff nicht möglich ist und dies durch das Zücken seines Presseausweises unterstrich. Anschließend gab es noch eine kleine Führung durch die neuen FoeBuD-Räume.

Staatsschutz und BKA waren sichtlich von der Ordentlichkeit beeindruckt, waren sie es doch schließlich gewohnt, sich bei MailBox-Durchsuchungen erst durch zugemüllte Hinterzimmer kämpfen zu müssen :)

Der Staatsanwaltschaft teilten die Beamten telefonisch ihren Erfolg mit. Ja, die Daten seien ein Beweis, erklärte der Polizist; als padeluun rechtlich präzisierte: "Ein schwächerer Anscheinsbeweis!", waren die Ermittler dann doch relativ baff.

Dann mußte man auch schon wieder aufbrechen, schließlich sollte auch noch der Autor des "Kleinen Terroristen" besucht werden. Zum Glück blieben sowohl er als auch seine Eltern (der chemisch begabte Wunderknabe war zur Tatzeit 17 Jahre alt) sehr ruhig. Die Ermittler wollten zwar keinen Tee von ihm, aber sonst lief alles freundlich ab. "Eine Sache fehlte ja noch bei dem Text: die Quellenangabe. Hier ist sie!", sagte der junge Bastler und drückte dem Staatsschutz sein Schul-Chemiebuch in die Hand...

Es geht weiter

Der Landesbeauftragte für Datenschutz der Hansestadt Bremen, Franz Werner Hülsmann, meldete sich gleich nach der Durchsuchung. In einem Rundschreiben an den Bundesbeauftragen und die Landesbeauftragten für Datenschutz sowie an seine zuständigen Senatoren wies er darauf hin, daß MailBoxen immerhin nach dem FAG dem Artikel 10 des GG unterliegen und somit nicht so ohne weiteres durchsucht werden können. Nur wenn die Vorrausetzungen des G10-Gesetzes erfüllt werden, kann eine MailBox durchsucht werden, da die privaten Mails und Userdaten schützenswert sind.

"Ich möchte Sie daher bitten", schrieb Hülsmann, "bei den zuständigen Stellen dauf hinzuwirken, daß künftig auch bei den privaten Betrei-

bern und Betreiberinnen von MailBoxen sowie deren Benutzern und Benutzerinnen das Fernmeldegeheimnis durch staatliche Stellen nicht verletzt wird".

Es ist ein Unding, daß hier BetreiberInnen von MailBoxen als Angeklagte angesehen werden, nicht als Zeugen. Im politischen Raum ist weiterhin ernsthaft darüber nachzudenken, inwiefern MailBoxbetreiber einer Schweigepflicht -- vergleichbar mit Pfarrerinnen und Ärzten -- unterliegen sollten. Immerhin bekommen sie an diesen Schnittstellen der Kommunikation weitaus mehr mit, als Senderinnen und Sendern von elektronischen Botschaften lieb sein kann.

Der Durchsuchungsgrund war jedoch geradezu grotesk: Die erwähnte Nachricht bestand aus einem Zitat (mit Quellenangabe) aus dem frei zugänglichen Roman "Buntspecht. Sowas wie eine Liebesgeschichte von Tom Robbins", der im Rowohlt Verlag erschienen ist. Die Ermittler gaben gegenüber Chris' Anwalt an, sie hätten zwar nach dem Roman gesucht, könnten sich allerdings nicht erinnern, in welchem Buchladen sie gefragt hätten. Daß das Verfahren eingestellt wird, ist zum jetzigen Zeitpunkt so gut wie sicher. Anderenfalls will Chris selbst rechtliche Schritte einleiten.

"Rueckruf Leitstelle Siemens betr. Stoerung im AKW"

Paranoia und Ungereimtheiten

Völlig unklar ist in diesem Zusammenhang die Rolle des Verfassungsschutzes. Es ist bekannt, daß das Bundesamt für Verfassungsschutz im Thule-Netz zumindest mitliest. Auch im Spinnen-Netz, einem Verbund von radikalen linken MailBoxen, war der VS durch Klaus Steinmetz, V-Mann und "Computerexperte" der RAF, beteiligt. Daß der VS beim Aufbau des SpinnenNetzes involviert war, gab der Präsident des Bundesamtes für Verfassungsschutz, Dr. Eckart Werthebach, Anfang dieses Jahres im Gespräch mit dem FoeBuD zu. Zitat Werthebach: "Ja, das ist doch unsere Aufgabe!"

Es ist zumindest zu vermuten, daß auch das Thule-Netz vom BfV benutzt wird. Daß bei politisch progressiven Systemen wie der //BIONIC und der LINK-GOE Hausdurchsuchungen erfolgen, die rechtsextremen Boxen jedoch tabu bleiben, könnte dadurch erklärt werden, daß das Thule-Netz als Privatexperiment des VS für normale Polizeieinheiten nicht freigegeben wird.

Hausbesuch wegen einer Liebesgeschichte

Neben dem "Kleinen Terroristen" war im Thule-Netz noch eine andere Nachricht aus /T-NETZ/PYROTECHNIK weitergeleitet worden. Es handelte sich um eine Beschreibung von improvisierten Sprengstoffen für den nächsten Gefängnisaufenthalt, die aus Joints, Apfelmusgläsern, Abflussreiniger und ähnlichen Sachen hergestellt werden können. Diese Nachricht kam aus dem Göttinger /CL-System LINK-GOE.

Am 3.5. 1994 schaute das BKA dann auch bei Chris Vogel, dem Betreiber der MailBox vorbei. Da Chris schon mit padeluun Kontakt aufgenommen hatte, verhielt er sich -- den guten Erfahrungen aus Bielefeld gemäß -- kooperativ gegenüber den Beamten.

Im Vorwort der BfV-Broschüre "Befugnisse, Aufgaben, Grenzen" schreibt Werthebach: "Der Schein ist nicht immer das Sein -- und manchmal ist es schwer, hinter Schlagworten, politischen Konzepten, gutem Willen und falschen Absichten das herauszufiltern, was Tatsache ist." Wie wahr! Anekdote am Rande: Ein Saarbrücker FoeBuD-Mitglied fragte beim BfV an, was von dem Buch "Das RAF-Phantom" zu halten sei. Als Antwort kamen aus Köln zwei fotokopierte Zeitungsartikel, einer aus der taz, der andere aus dem Neuen Deutschland, die zeigen sollten, daß im "RAF-Phantom" nur zwei Journalisten ihre Verschwörungstheorien pflegen. Wenige Tage später erfolgte dann eine Hausdurchsuchung bei den Autoren wegen der Veröffentlichung von Geheimmaterial...

Die Geschichte geht weiter. Die Hausdurchsuchungen in Bielefeld und Göttingen sind erst der Anfang einer neuen Phase der Beschäftigung von staatlichen Stellen mit dem erwachsen gewordenen Hackermedium MailBox. To be continued....

(Jens Ohlig, Bielefeld)

Filename BIELBULL.D47 Lastedit: 9405072140
Autor: JENS

The Internet Factor

In a computational tour de force that could affect the security of the information superhighway, a team of computer scientists has solved a long-standing mathematical problem: finding the prime factors of a 129-digit composite number.

When the puzzle was originally posed in 1977 by cryptographers trying to demonstrate the power of a new encryption system, scientists estimated it would take 40 quadrillion years to solve.

But by using the Internet to divide the numbercrunching task among 1,600 computers, a team of volunteers managed to crack the code in just eight months. Corporations and government may now have to shore up their systems for transmitting sensitive information.

TIME magazine, May 9, 1994.

Buch

"Anleitung zum politischen Ungehorsam", Hrsg. Bügerforum Paulskirche & Büro für notwendige Einmischungen Knaur Verlag, ISBN 3-426-80040-3

Kein Kochrezept, sondern eine Sammlung von Texten und Aktionsbeispielen bekannter und unbekannter politischer und nicht-ganz-so politischer Gruppierungen, Vereine und Einzelpersonen. Ein Aufruf gegen "Politikverdrossenheit" (das Wort des Jahres 1993) und politische Resignation. Beispiele dafür, was Mensch (noch) machen kann.

Wichtig: das Netzwerk-ABC, eine Sammlung von Gruppen, die sich einmischen. Adressen, Telefonnummern und Arbeitsbeschreibungen. Für alle, die mitmachen wollen und nicht wissen, was es schon alles gibt.

Isl4

The Clipper Chip War

Stell Dir vor, Du bist ein Geheimdienst und alle verschlüsseln ihre Daten und Du kommst nicht mehr dran. Was würdest Du tun?

In den USA hat sich die National Security Agency (NSA) folgendes überlegt: Entwickle einen Super-Verschlüsselungschip und laß' ihn überall einbauen. Natürlich muß der Chip eine Hintertür haben, durch die es staatlichen Orgenen möglich wird, doch noch an die Daten heranzukommen.

Die Antwort ist der sogenannte Clipper-Chip, welcher in der Lage ist, von Telefongesprächen bis Computerdaten alles zu verschlüsseln und zwar so, daß man schon ein bischen länger braucht um die Daten zu entschlüsseln als beim DES Verfahren.

Mit Hilfe der Regierung wird der Clipperchip nun so billig hergestellt, daß alle ihn einbauen werden. Angefangen bei den Regierungsstellen, die den Clipper-Chip zwangsverordnet bekommen, bis hin zu Firmenvorständen, die ja auch gern mal was Vertrauliches mit ihrer zuständigen Regierungsstelle besprechen wollen. Und zum Glück für die NSA und alle rechtschaffenden Menschen hat der Clipper-Chip auch eine Hintertür, durch die man, unter Verwendung eines Master-Keys - der natürlich aus Sicherheitsgründen z.B. zwischen Judikative und Exekutive aufgeteilt wird - alle bösen Menschen und Drogendealer abhören kann.

Das beruhigt doch. Oder beunruhigt. Denn wenn man diese Idee einmal näher betrachtet, verliert sie rasch an Boden.

Durchführbar ist dies allemal. Man stelle sich vor, alle Regierungsstellen benutzen, weil vorgeschrieben, den Clipper-Chip. Alle anderen, die sensible Daten haben auch - denn, wenn sich die Regierung den Chip erstmal teuer selbst verkauft hat, ist er billiger als das, was es sonst noch geben wird - außerdem ist man kompatibel zu einer ganze Menge Leute.

Eine Machbarkeitsstudie

Die NSA hört also alle ab, die sowieso nichts zu verbergen haben - denn wer echte Sicherheit will, setzt natürlich sein eigenes Sicherheitsverfahren obendrauf. Was hat sich also geändert? Immerhin kann mich mein Nachbar jetzt nicht mehr abhören. Was passiert also? Im schlimmsten Fall verbietet jetzt die Regierung den Einsatz von Verschlüsselungsverfahren, die nicht auf dem Clipper-Chip basieren. Dann haben wir plötzlich eine ganze Menge Kriminelle mehr.

Und dann kommt plötzlich einer und sagt: Ich habe das System geknackt. Der spinnt natürlich und es wird auch bald bewiesen, daß er es garnicht geknackt haben kann. Denn die schlauen Leute sitzen ja schon alle bei der NSA, sind nicht bestechlich, nicht erpressbar, nicht enttäuscht und nie betrunken. Außerdem weiß keiner genug. Aber DES war ja auch todsicher. Also, vielleicht hat es ja doch jemand geknackt? Wenn dieses Gerücht einmal zuviel Substanz bekommen sollte, kann man alle Telefone mit dem Clipper-Chip in die Tonne treten. Oder sie mit Flash-EPROMs ausrüsten und den Dämonen der Inkompatibilität zum Fraß vorwerfen.

Ein System mit Hintertür ist wie eine Bank mit offenem Klofenster, wenn man es gefunden hat, kann man alles damit machen. Und plötzlich wird die NSA abgehört. Oder bekommen die eine Sondergenemigung und benutzen ein Public-Key Verfahren? Ein Verfahren ohne Hintertür, bei dem jeder mit jedem Daten Luft- und Wasserdicht austauschen kann und wo der einzige Schwachpunkt in der Disziplin der Benutzer liegt?

Der Clipper-Chip ist so definitiv blödsinnig, daß man sich fragt, was damit eigentlich tatsächlich bezweckt werden soll. Denk Dir was.

lsl4

Käse aus Holland

Das neue Computerkriminalitätsgesetz in den Niederlanden

Seit dem 1. März 1993 hat die niederländische Justiz eine neue Waffe gegen Hacker, Phreaks und Computerkriminelle: den Straftatbestand der Computerkriminalität. Bisher musste auf Gesetze zurückgegriffen werden, in denen Computer nicht existent waren und deshalb oft nicht auf die veränderte Lage zutrafen.

Das niederländische Computerkriminalitätsgesetz setzt sich aus erneuerten alten und völlig neu erstellten Artikeln zusammen. Zum Beispiel kann Spionage jetzt offiziell per Computer betrieben werden. Das Abhören von Telefonleitungen kann zur Überwachung von Gesprächen und jetzt auch von elektronischer Datenübertragung eingesetzt werden.

Das neue Gesetz behandelt völlig neue Themen. Obwohl dort andere Begriffe verwendet werden, als Hacker sie normalerweise benutzen, erkennen wir doch einige Themen, die uns bekannt vorkommen. Beim Lesen dieses Artikels bitte bedenken, dass der reine Text eines Gesetzes noch keine Auskunft darüber gibt, was jetzt wirklich legal ist und was nicht. Das hängt immer noch zu einem grossen Teil davon ab, wie die Polizei, Richter und Staatsanwälte es interpretieren und damit umgehen. Das Gesetz ist noch sehr jung, und es gibt bis jetzt noch kaum Präzedenzfälle.

Hacking

Der Aufenthalt in einem Computersystem, zu dem man keine Zugangsberechtigung hat, ist verboten. Wenn, um in das System zu gelangen, ein Paßwort erraten, ein Trojanisches Pferd oder ein Passwort-Cracker verwendet wird oder der Account von jemand anderem benutzt wird, kann das maximal sechs Monate Gefängnis kosten, sofern man sich nur umsieht und nichts anfasst, verändert oder kopiert.

Für das Kopieren von Daten ist die Strafe weit höher: 4 Jahre. Das illegale Eindringen in ein System per Modem und die Nutzung dessen Prozessorkapazitäten für eigene Zwecke wird ebenso mit maximal 4 Jahren bestraft. In diesem Fall heisst das: man hat nur das System benutzt und nichts verändert, beschädigt oder kopiert.

Noch um einiges interessanter ist das nächste Verbrechen, das man begehen könnte: Eine Person, die mit ihrem Modem illegal auf ein System zugreift und dann von dort auf ein anderes System geht (die niederländische Gesetzgebung verwendet hier den Begriff "hopping"), muss ebenfalls mit 4 langen Jahren im Gefängnis rechnen. Auch wenn diese Person kein einziges Bit der von den Systemadministratoren so heiss geliebten Daten verändert, kopiert oder oder beschädigt. Die Straftat unterscheidet sich im Grunde nicht von der im ersten Absatz beschriebenen. Die Anwendung eines Modems jedoch ist offenbar der ganze Unterschied.

Aus irgendeinem Grunde sind Menschen mit Modems wohl um einiges suspekter als die, die keines besitzen.

Ein Silberstreif am Horizont ist allerdings zu sehen. Zwar ist es verboten, Informationen wie (Firmen-)Geheimnisse oder andere Daten, die einem durch Hacken oder auf andere Weise in die Hände geraten und die nicht zur Veröffentlichung bestimmt sind, zu verwenden oder zu veröffentlichen. Wenn aber eine Veröffentlichung dieser Inhalte im allgemeinen Interesse liegt, ist diese legal. In diesem Fall ist auch bei gehackten Informationen eine strafrechtliche Verfolgung des Hakkens selbst unwahrscheinlich.

Beschädigungen

Noch etwas, das speziell nicht erlaubt ist, ist das Beschädigen oder Stören der Funktionsfähigkeit eines Computersystems oder Teilen der Kommunikations-Infrastruktur. Darunter fällt alles vom Verändern einiger Bytes in einem Computersystem bis zum physikalischen Abbrennen einer Vermittlungsstelle. Die verhängte Strafe hängt von der Grösse des entstandenen Schadens ab und variiert von 6 Monaten bis zu 15 Jahren. Die 15 Jahre werden nur dann verhängt, wenn Menschen ums Leben gekommen sind, zum Beispiel, wenn das Computersystem eines Krankenhauses manipuliert wird oder die Telekommunikationseinrichtungen einer Notrufannahme gestört werden.

Illegales und absichtliches Verändern, Hinzufügen oder Löschen von Daten in einem Computersystem kann mit bis zu 2 Jahren Gefängnis bestraft werden. Wenn jedoch über Modem illegal in einen Computer eigedrungen wird und den vorhandenen Daten ernster Schaden zugefügt wird, beträgt die Höchststrafe 4 Jahre. Wer also vorhat, schwere Schäden zu verursachen, sollte dies lieber direkt an der Konsole tun. Das Risiko, erwischt zu werden, ist zwar höher, aber die maximale Strafe nur halb so hoch. Auch hier sind Personen, die Modems benutzen, der Gesetzgebung offenbar unheimlich.

Damit zu drohen, zum eigenen Nutzen Daten auf einem System zu zerstören oder das System zu crashen (einfache Leute nennen das wohl Erpressung), kann bis zu 9 Jahren Gefängnis bedeuten. Diese Strafe kann sich auf 12 Jahre ausweiten, wenn die Straftat von zwei oder mehr Beteiligten begangen wird, nachts in einer Wohnung, auf offener Strasse oder im Zug (der Gesetzesartikel, der in diesem Fall die Strafe festlegt, ist ursprünglich für Diebstahl mit Gewalt oder Drohung konzipiert. Mit etwas Phantasie kann er also auch auf mobile Computerkriminelle mit Laptop und Funktelefon angewendet werden). Wenn dabei ein Mensch ums Leben kommt, kann die Strafe bis zu 5 Jahren betragen.

Viren

Es ist verboten, Daten, die den Zweck haben, sich selbst zu reproduzieren, in Computersystemen zu verbreiten. Personen, die dies illegal und absichtlich tun, riskieren, für 4 Jahre ins Gefängnis zu gehen. Falls ein Virus unabsichtlich verbreitet wird, beträgt die maximale Strafe einen Monat. Zum Zwecke der Aufklärung ist es gestattet, Viren zu verteilen, um von Viren verursachte Schäden vermeiden zu können. Niederländische Virenfreaks spekulieren noch, ob es sicher ist, zu Zwecken der Weiterbildung untereinander Viren auszutauschen. Bis jetzt ist in den Niederlanden noch niemand wegen eines Virus in Schwierigkeiten gekommen.

Phreaking

Die Nutzung öffentlicher Telekommunikationseinrichtungen unter Anwendung technischer Tricks oder falscher Signale mit dem Ziel, dafür nicht oder nur teilweise bezahlen zu müssen, kann bis zu 3 Jahren Gefängnis bedeuten. Man könnte sich jetzt eine ganze Reihe technischer Tricks vorstellen, von kultiviertem Blueboxing bis zum Mißbrauch der nachbarlichen Telefonleitung. Was aber "falsche Signale" sein sollen, hat bis jetzt noch niemand herausgefunden. Diese seltsame Formulierung riss einen niederländischen Phone phreak zu der entrüsteten Bemerkung hin: "Wie jetzt - falsche Signale? Ich verwende nur richtige Signale!"

So wie dieser Gesetzesartikel geschrieben ist, könnte er auch bedeuten,

dass es legal ist, Einrichtungen zu benutzen, die der Öffentlichkeit nicht oder noch nicht zugänglich sind. Die hardcore phreaks werden also möglicherweise nicht gezwungen werden, ihr Hobby an den Nagel zu hängen. Hier muss man allerdings richtig gut sein, das niederländische Telefonsystem ist nämlich ziemlich modern und es ist nicht so ganz einfach, damit herumzuspielen.

Das Verkaufen und Verbreiten von und Werben für Blueboxen, Software oder anderen Daten, die für das Phone phreaking von Bedeutung sind, kann mit einem Jahr Gefängnis bestraft werden. Das könnte auch bedeuten, dass Phone phreaks beim Austauschen der neuesten Tricks vorsichtig sein müssen. Wer Derartiges verkauft, verbreitet oder dafür wirbt, kann für 3 Jahre eingesperrt werden.

Social Engineering

Wenn eine Person von jemandem Informationen bekommt, die nicht für ihre Augen, Ohren oder Disketten bestimmt sind, in dem sie diesen Menschen in die Irre führt oder vorgibt, jemand anderes zu sein, betreibt sie, je nach Art der Information, social engineering. Das kann mit bis zu 3 Jahren bestraft werden. Interessant übrigens, dass der Artikel in einem Gesetz zur Computerkriminalität zu finden ist...

Datenempfang

Natürlich ist es verboten, anderer Leute Voice- oder Daten-Telefonleitungen abzuhören. Alles, was durch die Luft geht, darf frei empfangen werden. Seit dem 1.1.93 ist es für den Fall, daß man dabei besonderen Aufwand betreibt, verboten, Daten unbefugt über Funk zu empfangen. Was unter "besonderem Aufwand" zu verstehen ist, ist noch vollkommen unklar. Möglicherweise ist es illegal geworden, Pager-Informationen (Cityruf) zu empfangen, die mit ein wenig Elektronik ziemlich leicht auf den heimischen Bildschirm zu bekommen sind. Wie auch immer, solange, bis jemand dafür verhaftet wird, können wir nur spekulieren.

Karten

Das Verfälschen oder das Erstellen falscher Bankkarten, Kreditkarten und ähnlicher Dinge zum eigenen Vorteil ist nicht gestattet. Das bedeutet wahrscheinlich: Wer Karten kopiert oder seine eigenen Daten auf eine Blankokarte schreibt, um reich zu werden, riskiert maximal 6 Jahre seines jungen, kostbaren Lebens. Möglich ist auch, dass das Kopieren oder Erstellen von Karten, nur aus Interesse an der Technik, legal ist.

Dieselbe Strafe erwartet jeden, der eine gefälschte Karte benutzt, als wäre sie echt und nicht gefälscht. In diesem Fall sagt das Gesetz nicht ein Wort über erschlichene Vorteile. Also geht der Hacker, der eine Kopie seiner Karte macht und sie ausprobiert, nur um zu sehen, ob es funktioniert, für bis zu 6 Jahre ins Gefängnis!

Das Leben, die Gesetze und der ganze Rest

Das Computerkriminalitätsgesetz wurde laut den Erstellern hauptsächlich konzipiert, um richtige Computerkriminelle ins Netz zu bekommen. Den Bankangestellten, der seine Firma um Millionen betrügt, den Rache schwörenden Ex-Systemverwalter, der damit droht, das System der Firma, die ihn gefeuert hat, zu crashen, oder den harten Kriminellen, der mit grossen Mengen gefälschter Kreditkarten handelt. Es wurde nicht speziell für die vielleicht irritierenden, aber letztendlich kleinen, Hacker im System entworfen.

Soweit die Ersteller...

Innerhalb von drei Wochen nach dem berüchtigten 1.März verhaftete die Amsterdamer Polizei das erste Opfer des neuen Gesetzes: der neunzehnjährige Hacker RGB wurde verhaftet, als er an einem Unix-System der Freien Universität Amsterdam sass. RGB, der kein Student dieser Uni ist, wurde verdächtigt, sich unter dem Account von jemand anderem eingeloggt zu haben und vom Amsterdamer System aus eine Verbindung zum System der Technischen Universität von Delft aufgebaut zu haben, das sich ebenfalls in den Niederlanden befindet.

Nach dem neuen Gesetz hätte er dafür für bis zu 4 Jahre ins Gefängnis gehen können. RGB wurde 38 Tage in Untersuchungshaft festgehalten, obwohl er die Aussage verweigerte. Wegen des offensichtlichen Mangels an Beweisen wurde er dann freigelassen und hat seitdem nicht mehr viel von den zuständigen Behörden gehört. Momentan erscheint eine strafrechtliche Verfolgung seines vermuteten digitalen Grenzüberschritts nicht mehr sehr wahrscheinlich.

Die Folgen

Was sind die Auswirkungen des neuen Gesetzes auf die niederländische Hack- und Phreak-Gemeinde?

Also, eins ist sicher: Einige Hacker hacken seit dem 1. März nicht mehr. Die, die es noch tun, sind ziemlich vorsichtig geworden, wenn es darum geht, anderen davon zu erzählen. Die Leute tauschen jetzt Informationen aus, "um andere vor den Sicherheitsrisiken bestimmter Systeme zu warnen". Oder sie sagen: "Hey, ich habe da irgendwo etwas Interessantes gehört - aber probier es nicht aus, es ist illegal." Nur sehr wenige, nicht-so-schlaue Mitmenschen behaupten manchmal, sie hätten dies oder das gehackt. Meist glaubt ihnen niemand. Die niederländischen Phreaks, die den Demon Dialer, das perfekte Phone-phreak-Werkzeug, gebaut haben, haben wegen dieses Gesetzes damit aufgehört, ihn zu verkaufen. Hack-Tic, die einzige niederländische Hackerzeitung, wird in Zukunft nicht mehr über grosse Hacks in Konzerne u. ä. berichten. Oh, natürlich könnten sie die Informationen als anonymous mail bekommen... ;-)

Aber nicht alles ist verloren. Im August 1993, 5 Monate nach der Verabschiedung des Computerkriminalitätsgesetzes, war es immerhin möglich, in den Niederlanden einen dreitägigen internationalen Hackerkongress mit ca. tausend Teilnehmern aus 15 verschiedenen Ländern zu organisieren. Einerseits redeten die Leute dort in aller Offenheit über Hacking und Phreaking, obwohl das meiste, wovon die Rede war, vor dem 1.3.93 stattgefunden hatte. Andererseits konnte man bereits einen Interessenwandel bemerken - vom "Hacken als Selbstzweck" hin zu den Einflüssen der Computertechnologie auf die Gesellschaft.

Diese Entwicklung wird sich wohl in Zukunft fortsetzen. Hacker sind nicht nur an Technik interessiert, oder daran, böse oder illegale Dinge zu tun. Sie sind lediglich Leute, die Sachen wissen und ausprobieren wollen, die neue, ungewöhnliche und kreative Ideen aufbringen. Sie sind Leute, die ihre Augen nicht vor den Einflüssen neuer Technologien auf die Gesellschaft verschliessen, sondern diese kritisch beäugen. Und egal, was in Zukunft auch für Gesetze eingeführt werden: es wird immer neue Interessengebiete geben, die von kreativen Köpfen erforscht werden können...

Hanneke Vermeulen

CHAOS-B - Chaos Computer Club Berlin Treffen jeden Dienstag ab 20 Uhr im Clubraum in der Kronenstr. 3, Berlin-Mitte (U-2 oder 6: Stadtmitte) im dritten Stock über dem Friseur (Eingang links davon).

CHAOS-HL - Chaos Computer Club Luebeck Treffen am ersten und dritten Freitag im Monat um 19 Uhr in der Roehre (gerade Querstrasse, geht von der Mengstrasse ab). Voice +49-451-31642, Mbx MAFIA +49-451-31642 Briefpost: CCC-HL, c/o Benno Fischer, Bugenhagenstr. 7, Lübeck

CHAOS-RH - Chaos Computer Club Recklinghausen Treffen alle zwei Wochen oder auch nicht. Voice +49-2364-16349, Fax +49-2361-652744 Mailbox: LITB +49-2363-66378 / LIVETIMES +49-2361-373214

CCC-Ulm - Chaos Computer Club Ulm Treffen jeden Mittwoch, 19 Uhr im Cafe "Einstein", Uni-ULM Kontakt: Framstag, framstag@rz.uni-ulm.de (Ulli Horlacher, Landfiedbühl 5, 7900 Ulm) und Deep Thought (brenner@tat.physik.uni-tübingen.de) (Martin Brenner) oder CCC-ULM, ccc-ulm@sol.zer und ccc-ulm@sol.north.de

CHAOS-RN - Chaos Computer Club Rhein Neckar Treffen jeden Dienstag 20 Uhr im "Vater Rhein" in HD. Von der Stadthalle über die Fussgängerampel, durch den Minipark, halb links, rein, hinterer linker Flügel der Gaststätte. Mailbox CHAOS RN unter +49-6221-904727 Briefpost: CCC-RN, Postfach 104027, W6900 Heidelberg

SUECRATES - Stuttgarter Computerrunde mit Zeitschrift D'Hacketse Kontakt: T.Schuster, Im Feuerhapt 19, W7024 Filderstadt 3 E-Mail: norman@delos.stgt.sub.org

2600 USA - 2600 Magazine - the quarterly journal of the american Hacker Overseas $30 individual, $65 corporate Back issues available for 1984-88 at $25 per year, $30 per year overseas. Adress all subscription correspondence to: 2600 subcription dept, P.O. Box 752, Middle Island, NY 11953-0099 Voice: +1-516-751-2600 / Fax-Line: +1-516-751-2608 Voice-Mail-System: +1-516-751-6634

2600 München - 2600 Meeting in Germany Jeden ersten Freitag im Monat um 18:00 Uhr im Münchener Hauptbahnhof in der ersten Etage bei Würger King und den Telefonzellen. Erreichbar als 2600@sectec.hanse.de, Voice-Mailbox +1-904-366-4431, auf den Treffen im Hauptbahnhof ueber die anrufbaren Zellen +49-89-591-835 und +49-89-558-541 (bis 545, hier handvermittelt über Operator).

FoeBud - Verein zur Foerderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. Bielefeld Treffen jeden Dienstag, 19:30 Uhr im Cafe "Spinnerei", Heeperstr. 64, Bielefeld, dort voice 49-521-62339 Voice +49-521-175254, Fax +49-521-61172 Mailbox BIONIC unter +49-521-68000 Briefpost: FoeBuD, Marktstr. 18, W4800 Bielefeld e-mail: ZENTRALE@BIONIC.ZER / zentrale@bionic.zer.de

Hack-Tic - Tijdschrift for techno-anarchisten Briefpost: Postbus 22953, NL-1100 DI Amsterdam Voice: +31-20-6001480 / Fax: +31-20-6900968

Impressum

Die Datenschleuder,
das wissenschaftliche Fachblatt für Datenreisende.

- Ein Organ des Chaos Computer Club -

Nummer 47, Quartal II, Mai 1994

Adresse: Schwenckestraße 85 D-20255 Hamburg 20, Tel. +49-40-4903757, Fax +49-40-4917689, Mailbox +49-40-4911085, Voice-Mail +49-40-497273 (Tonwahl), Internet/UUCP ccc@t42.ccc.de, Bildschirmtext *CCC#

Redaktion: (A)ndy M.-M., Christine, Konny, Hacko, Wau Holland, Hanneke, Jens Ohlig, padeluun, rowue, Maku, Poetronic, Rosa, RON

Beiträge, Informationen, auch Kurzmeldungen bitte zur Sicherheit immer auch schriftlich einschicken.

ViSdPg: Andy Müller-Maguhn

Herausgeber: Chaos Computer Club e.V.

Druck: St. Pauli Druckerei, Hamburg St. Pauli

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder.

Einzelpreis 3,50 DM. Mitglieder des Chaos Computer Club e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft. Abopreis → Bestellfetzen.

(Clopyright 1994: Alle Rechte bei den AutorInnen. Kontakt über die Redaktion.

Nachdruck für nichtgewerbliche Zwecke mit Quellenangabe erlaubt. Belegexemplar erbeten. Eigentumsvorbehal: Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechts-mittelfähigen Bescheides zurückzusenden.

Vorname _____ Straße _____

Name _____ Ort _____

Telefon _____

(freiwillig)

BRESTELLFETZEN... bitte ausgefüllt senden an den
Chaos Computer Club * Schwenckestrasse 85 * D-20255 Hamburg
Telefax +49-(0)40-4917689
Mitgliedschaft im CCC e.V. (Die Mitgliedschaft schließt ein Datenschleuder-Abo ein)

	mvsat	1.00 DM	Satzung des Chaos Computer Club e.V.
	mvein	20.00 DM	Einmalige Verwaltungsgebühr bei Eintritt
	mvsoz	60.00 DM	Mitgliedsbeitrag, Sozialtarif
	oder	5.00 DM	monatlich (Dauerauftrag)
	mvnrm	120.00 DM	Mitgliedsbeitrag, Normaltarif
	oder	10.00 DM	monatlich (Dauerauftrag)
	Datenschleuder Abonemment		
	dssoz	30.00 DM	Abonemment, Sozialtarif
	dsnrm	60.00 DM	Abonemment, Normaltarif
	Bücher		
	habi1	33.33 DM	Die Hackerbibel, Teil 1 (260 Seiten A4)
	habi2	33.33 DM	Die Hackerbibel, Teil 2 (260 Seiten A4)
	Diverses		
	stud	7.50 DM	CCC-Studie für die Grünen, Computereinsatz im Bundestag
	mutst	16.00 DM	Elektronische Informationssysteme für den Umweltschutz
	doku	5.00 DM	Dokumentation zum Tod von "KGB-Hacker" Hagbard (Karl Koch)
	zerb	20.00 DM	Zerberus BenutzerInnen-Handbuch
	Disketten		
	crypt	25.00 DM	Sammlung von Verschlüsselungsprogrammen, PGP + Handbuch
	hack	25.00 DM	PC-Soundprogramm für blaue Töne & POCSAC-Decoder mit Dokumentation - nur für Schulungszwecke
	Aufkleber		
	3ks	3.33 DM	3 Aufkleber Chaos-Knoten "Kabelsalat ist gesund"
	oah	3.33 DM	Restposten: 64 Aufkleber "Achtung Abhörgefahr" in alt-Post-gelb zum Selberausschneiden
	ah	5.00 DM	15 Aufkleber "Achtung Abhoergefahr" postmoderngrau
	ooo	5.00 DM	Bogen mit Post-Totenkopf-Aufklebern verschiedener Größe
	glob	5.00 DM	Bogen m. 10 Klebern "Globales Dorf, rechtsfreier Raum"
	zula	5.00 DM	Bogen mit Zulassungszeichen ("ZZF-Prüfnummer")
	cia	5.00 DM	Selbstausschneiden: 64 Kleber "Chaos im Äther - ich höre zu"
	Allgemein		
5.-	Portopauschale		
	Der Sozialtarif gilt für Schüler, Studenten und ähnlich minder Betuchte.		
	Da unser Versandpersonal ehrenamtlich tätig ist, bitten wir um Verständnis für Lieferzeiten bis zu max. 6 Wochen.		
			Gesamtbetrag, liegt der Bestellung in
		bar	
		PWZ (1.-)	Congress-Doku (CCC-94) 15.-
		V-Scheck	Doku ueber Lockpicking 50.-
	bei, bzw.		
		wurde am	überwiesen auf Kto. 59 90 90 - 201 bei der Postbank HH (BLZ 20010020)

Eingang: _____ Betrag erhalten: _____ Erledigt: _____